In the Claims:

1. (Currently Amended) An adder circuit for summing a plurality of addends from multi-bit words comprising:

a network of n-input carry-save adder circuits each having a first number of sum outputs and a second number of carry outputs, the adder circuits being arranged in a plurality of columns each column corresponding to a predetermined bit position in the sum, and being arranged in a plurality of levels,

the first level receiving a number of addends from corresponding bit positions of selected ones of the plurality of words and the lower levels each receiving addends from one or more of (i) corresponding bit positions of other selected ones of the plurality of words, (ii) sum outputs from a higher level adder circuit in the same column, and (iii) carry outputs from a higher level adder circuit in a column corresponding to a less significant bit position, at least one of the levels receiving addends corresponding to a calculation involving another one of the words,

wherein the number of n-input adders in each column varies according to the bit position.

2. (Original) The circuit of claim 1 in which the number of n-input adders in each column is specifically adapted to the number of addends required for that column.

3. (Original) The circuit of claim 1 in which the number of n-input adders in each bit position of the first level does not exceed the integer part of the number of addends divided by n.

4. (Previously presented) The circuit of claim 1 in which the number of n-input adders in each bit position of the lower levels does not exceed the integer part of:

the total of: (a) the number of sum outputs of the n-input adders in a higher level and the same column, (b) the number of unconnected inputs from a higher level and the same column, and (c) the number of carry outputs from a higher level and a column corresponding to a less significant bit position, which total is divided by n.

5. (Original) The circuit of claim 4 in which the number of unconnected inputs is that of the immediate higher level.

6. (Original) The circuit of claim 4 in which the number of sum outputs is that of the immediate higher level.

7. (Original) The circuit of claim 4 in which the number of carry outputs is that of the immediate higher level.

8. (Previously presented) The circuit of claim 1 in which n is three, and the first number of sum outputs is less than three and equal to the second number of carry outputs.

9. (Original) The circuit of claim 1 further including means for delivering each one of the plurality of multi-bit words to the network of n-input adders such that the number of addends per bit position varies as a function of bit position.

10. (Previously presented) The circuit of claim 1 further including one or more input adders placed at selected positions within the network.

11. (Original) The circuit of claim 10 in which the selected positions are determined so as to reduce the number of levels required to sum the plurality of addends.

12. (Previously presented) The circuit of claim 11 in which the n-input adders are three-input adders, the input adders are two-input adders, and in which each selected position is determined according to an identified bit position and level where the number of outputs would otherwise be greater than two, the selected position being at a level above the identified position and in the same bit position.

13. (Previously presented) An adder circuit comprising:

an input for receiving a plurality of addends;

first summation means for summing a plurality of addends to produce an output comprising a high order part and a first and second low order part;

a first feedback line for coupling the first high order part to a lower order position at said input, for a subsequent calculation;

an output stage including second summation means for summing the first and second low order parts to provide a first word output and a feedback register for retaining a carry bit from said second summation means and for providing said carry bit as input to said second summation means during a subsequent calculation.

14. (Original) The adder circuit of claim 13 in which the high order part comprises a sum term and a carry term fed back to a subsequent calculation.

15. (Currently Amended) The adder circuit of claim 13 in which the carry bit is used at the end of a subsequent calculation of the first and second low order parts that are calculated by the first summation means.

16. (Previously presented) The adder circuit of claim 13 for summing a plurality of addends from multi-bit words in which:

the first summation means comprises a network of carry-save adder circuits each having a number of inputs, a number of sum outputs and a number of carry outputs,

the adder circuits being arranged in a plurality of columns, each column corresponding to a predetermined bit position in the sum, and being arranged in a plurality of levels,

the first level coupled for receiving a number of addends from corresponding bit positions of selected ones of the plurality of words and the lower levels coupled for receiving addends from one or more of (i) corresponding bit positions of other selected ones of the plurality of words, (ii) sum outputs from a higher level adder circuit in the same column, and (iii) carry outputs from a higher level adder circuit in a column corresponding to a less significant bit position,

the first feedback line coupling a first plurality of more significant bit outputs of the lowest level Wadder circuits, as said first high order part, to a corresponding number of less significant bit inputs of said first level of adder circuits at said lower order position.

17. (Previously presented) The adder circuit of claim 13 in which the high order part comprises a high order carry term output and a high order sum term output, and in which the first low order part comprises a low order carry term output and the second low order part comprises a low order sum term output.

18. (Previously presented) A pipelined adder circuit for summing a plurality of addends from multi-bit words comprising:

first summation means comprising a network of carry-save adder circuits, the adder circuits being arranged in a plurality of columns, each column corresponding to a predetermined bit position in the sum, and being arranged in a plurality of levels the first level coupled for

receiving a number of addends from corresponding bit positions of selected ones of the plurality of words and the lower levels coupled for receiving addends from one or more of (i) corresponding bit positions of other selected ones of the plurality of words, (ii) sum outputs from a higher level adder circuit in the same column, and (iii) carry outputs from a higher level adder circuit in a column corresponding to a less significant bit position,

a first feedback line for coupling a first plurality of more significant bit outputs of the lowest level adder circuits to a corresponding number of less significant bit inputs of an intermediate level of adder circuits for a subsequent calculation, the intermediate level being between said first and lowest level adder circuits.

19. (Original) The pipelined adder circuit of claim 18 further including an output stage including second summation means for summing first and second low order parts respectively comprising a second and a third plurality of less significant bit outputs of the lowest level adder circuits to provide a first word output and a feedback register for retaining a carry bit from said second summation means and for providing said carry bit as input to said second summation means during a subsequent calculation.

20. (Cancelled).

21. (New) The circuit of claim 1, further including an integer-splitting block that splits each of at least two integers into the multi-bit words.

22. (New) The circuit of claim 1, further including an integer-splitting block that splits each of at least two integers into the multi-bit words for generating intermediate results used in executing cryptographic functions, and

wherein, for at least one of the multi-bit words, at least one of the lower levels receives an addend corresponding to a bit position from a different one of the multi-bit words.

23. (New) The circuit of claim 1, further including a feedback circuit configured to provide the addends corresponding to a calculation involving another one of the words.

24. (New) The circuit of claim 1, further including a feedback circuit configured to provide a feedback output from one of the levels for one of the words, to a previous level for a subsequent calculation involving another one of the words.

25. (New) The circuit of claim 1, wherein the network is configured to concurrently process at least two words, and

further including a feedback circuit configured to provide a feedback output from one of the levels for a calculation involving one of the words, to an intermediate level below a highest level for use as an intermediate input to a subsequent calculation involving a different one of the words.